CLAIMS

What is claimed is:

1. A method for generating transcodable encrypted content that comprises independently processable components, said method comprising:

accessing transcodable content that comprises independently processable components to be encrypted; and

encrypting at least one of said independently processable components to provide independently processable components which are independently decryptable, said encrypting performed using an encryption scheme that utilizes non-repeating identifiers that uniquely correspond to said independently processable components, wherein said transcodable encrypted content is transcodable without requiring knowledge of said encryption scheme.

2. The method as recited in Claim 1 wherein said independently processable components comprise components that are independently decodable and independently authenticatable.

3. The method as recited in Claim 1 wherein said encryption scheme comprises applying block ciphers in stream cipher mode.

4. The method as recited in Claim 1 wherein said encryption scheme comprises counter (CTR) mode stream cipher encryption.

5. The method as recited in Claim 1 wherein said encryption scheme comprises encrypting a counter to generate a keystream which is logically combined with plaintext to generate ciphertext.

6. The method as recited in Claim 1 wherein said encryption scheme utilizes non-repeating identifiers which are non-repeating counter values.

7. The method as recited in Claim 1 wherein said encryption scheme comprises performing several encryptions in parallel.

8. The method as recited in Claim 1 wherein differentiating metadata that corresponds to said independently processable components is used as an input to said encryption.

9. The method as recited in Claim 1 wherein said transcodable encrypted content has information associated with it to direct transcoding.

10. The method as recited in Claim 1 said transcodable encrypted content comprises respective components that have respective encryption keys, wherein said respective encryption keys are related to a root encryption key.

11. The method as recited in Claim 1 wherein said encryption scheme is selected from the group consisting of a block cipher used in output feedback (OFB) mode, RC4, SEAL, and WAKE.

12. A method for transcoding transcodable encrypted content that comprises independently processable components comprising:

accessing transcodable encrypted content that has been encrypted using non-repeating identifiers that uniquely correspond to said independently processable components such that said independently processable components are independently decryptable, and

transcoding said transcodable encrypted content without requiring knowledge of the encryption scheme used to encrypt said independently processable components.

13. The method as recited in Claim 12 wherein said independently processable components comprise components that are independently decodable and independently authenticatable.

14. The method as recited in Claim 12 wherein said encryption scheme comprises applying block ciphers in stream cipher mode.

15. The method as recited in Claim 12 wherein said encryption scheme comprises counter (CTR) mode stream cipher encryption.

16. The method as recited in Claim 12 wherein said encryption scheme comprises encrypting a counter to generate a keystream which is logically combined with plaintext to generate ciphertext.

17. The method as recited in Claim 12 wherein said encryption scheme utilizes non-repeating identifiers which are non-repeating counter values.

18. The method as recited in Claim 12 wherein said encryption scheme comprises performing several encryptions in parallel.

19. The method as recited in Claim 12 wherein differentiating metadata that corresponds to said independently processable components is used as an input to said encryption.

20. The method as recited in Claim 12 wherein said transcoding produces transcodable encrypted content that is smaller in size than the transcodable encrypted content that is accessed.

21. The method as recited in Claim 12 wherein said transcodable encrypted content has information associated with it to direct transcoding.

22. The method as recited in Claim 12 said transcodable encrypted content comprises respective components that have respective encryption keys, wherein said respective encryption keys are related to a root encryption key.

23. The method as recited in Claim 12 wherein said encryption scheme is selected from the group consisting of a block cipher used in output feedback (OFB) mode, RC4, SEAL, and WAKE.

24. A transcodable encrypted content generator for generating transcodable encrypted content that comprises independently processable components, said transcodable encrypted content generator comprising:

an accessor for accessing transcodable encrypted content that comprises independently processable components to be encrypted; and

an encryptor coupled to said accessor for encrypting at least one of said independently processable components to provide independently processable components which are independently decryptable, said encryptor further comprising:

a non-repeating identifier engine that produces non-repeating identifiers that uniquely correspond to said independently processable components; and

an output coupled to said encryptor, said output outputting transcodable encrypted content which is transcodable without requiring knowledge of an encryption scheme used by said encryptor to encrypt said at least one of said independently processable components.

25. The transcodable encrypted content generator of Claim 24 wherein said accessor is configured to access independently processable components that are independently decodable and independently authenticatable.

26. The transcodable encrypted content generator of Claim 24 wherein said encryptor comprises:

a block-stream cipher engine that applies block ciphers in stream cipher mode.

27. The transcodable encrypted content generator of Claim 24 wherein said encryptor comprises:

a counter (CTR) mode stream cipher encryptor.

28. The transcodable encrypted content generator of Claim 24 wherein said encryptor further comprises:

a keystream engine which encrypts a counter to generate a keystream; and

a combiner coupled to said keystream engine, said combiner configured to logically combine said keystream with plaintext to generate ciphertext.

29. The transcodable encrypted content generator of Claim 24 wherein said non-repeating identifier engine is configured to produce non-repeating identifiers which are non-repeating counter values.

30. The transcodable encrypted content generator of Claim 24 wherein said encryptor is configured to perform several encryptions in parallel.

31. The transcodable encrypted content generator of Claim 24 wherein said encryptor further comprises:

a differentiator which accesses differentiating metadata that corresponds to said independently processable components and associates the differentiating metadata with the independently processable components.

32. The transcodable encrypted content generator of Claim 24 wherein said transcodable encrypted content has information associated with it to direct transcoding.

33. The transcodable encrypted content generator of Claim 24 wherein said transcodable encrypted content comprises respective components that have respective encryption keys, wherein said respective encryption keys are related to a root encryption key.

34. The transcodable encrypted content generator of Claim 24 wherein said encryption scheme is an encryption scheme selected from the group consisting of a block cipher used in output feedback (OFB) mode, RC4, SEAL, and WAKE.